Til
Datatilsynet
post@datatilsynet.no

Oslo 10.05.2016

Klage på mobilapplikasjonen Runkeeper

Forbrukerrådet ønsker med dette å klage på følgende forhold knyttet til mobilappen Runkeeper:

1) Runkeeper sporer brukere og sender personopplysninger til tredjepart når den ikke er i bruk.
2) Appen ser ikke ut til å slette personopplysninger rutinemessig eller når bruker ber om det.

Vi ber Datatilsynet vurdere om appen Runkeeper som eies av selskapet FitnessKeeper Inc., er innrettet i tråd med norsk og europeisk personvernlovgivning og hvilke muligheter tilsynet har for inngripen.

FitnessKeeper Inc. er et amerikansk selskap med base i Massachusetts[1]. Etter det vi kjenner til har selskapet ikke etablert noe selskap eller representasjon i Europa[2]. Selskapet FitnessKeeper Inc. er ikke registrert under Safe Harbour[3].

Selskapet FitnessKeeper, Inc, leverer Runkeeper som er en applikasjonstjeneste (app). FitnessKeeper, Inc. tilbyr sine tjenester i et globalt marked, herunder det europeiske og det norske markedet og selskapet har tilknytning til Europa gjennom at selskapet retter sine tjenester mot det europeiske markedet.

Appen er tilgjengelig i et globalt marked, herunder det europeiske og det norske markedet. I fravær av tilknytning til Europa, utover at Runkeeper er tilgjengelig i disse markedene, ser vi at tilsynsmyndighetenes mulighet for sanksjoner kan være noe begrenset. Likevel forstår vi det slik at tilsynet i enkelte tilfeller kan se nærmere på en sak som den foreliggende. Forbrukerrådet anmoder derfor om at Datatilsynet benytter tilgjengelige kanaler for å undersøke saken og å løfte frem problemstillingene den reiser.

[1] FitnessKeeper, Inc., 2, 60 Canal St, MA 02114, USA
[2] FitnessKeeper eies av det japanske selskapet Asics som er mest kjent for produksjon av treningssko. Asics har representasjon i Europa.
[3] https://safeharbor.export.gov/list.aspx

Bakgrunn for henvendelsen

Forbrukerrådet har undersøkt brukervilkår og personvernpolicy i 20 ulike apper og presenterer dette i en rapport[4] som gir et bredt faktagrunnlag for ulike app-segmenter. I undersøkelsen ser vi nærmere på enkelte/ utvalgte sider ved brukervilkår og personvernpolicy til appene som er av stor betydning for den enkelte bruker. Undersøkelsen benyttet europeisk lovgivning som mal for sammenligning og vurdering.

I forbindelse med gjennomgangen av brukervilkår og personvernpolicy gjennomførte SINTEF på oppdrag fra Forbrukerrådet en test for å undersøke den faktiske dataflyten fra appene og om den enkelte app-tilbyder handler i tråd med egen personvernpolicy[5]. SINTEF testet dataflyten både da appene var i bruk og da telefonen ikke var i bruk i 48 timer (den såkalte 48-timerstesten). Det er spesielt tre apper hvor vi mener at SINTEF påviste brudd på personvernerklæringer eller vilkår[6]. Det er Vipps som Datatilsynet er i kontakt med allerede, Happn som den franske datatilsynsmyndigheten har fått en henvendelse på, samt Runkeeper, som vi med dette klager inn for Datatilsynet.

Forbrukerrådets rapport viser at mange apper, inklusive Runkeeper, er uklare på hva de definerer som personopplysninger. Mange apper, inklusive Runkeeper, ber om urimelig vide tilganger sammenlignet med hvilke tilganger som er nødvendige for å levere tjenesten. Vi ser også at mange apper, inklusive Runkeeper, betinger seg en varig rett til brukers innhold som også omfatter å dele brukeres innhold med uspesifiserte tredjeparter. Som mange andre apper kan kan også Runkeeper endre personvernpolicy uten å varsle bruker på forhånd. Sett i sammenheng med omfattende rett til brukerinnhold fremstår det som et urimelig avtalevilkår[7]. Et annet forhold vi ser i flere apper, herunder Runkeeper, er at tjenestetilbyderne ikke ser ut til å slette personopplysninger når appen ikke har vært i bruk på en tid, og heller ikke ser ut til å slette opplysninger om bruker sletter sin brukerkonto.

Om Runkeeper

Runkeeper er en treningsapplikasjon. Bruker kan eksempelvis holde oversikt over hvor fort en selv og ens venner løper og se avstander og kart for egnes og andres treningsøkter. I tillegg kan bruker integrere appen mot andre apper, som Facebook og Spotify samt med fitnessarmbånd som Fitbit[8].

Tjenesten er svært populær globalt og skal ha om lag 45 millioner brukere. Runkeeper er blant de mest populære treningsappene i Norge[9], uten at vi har eksakte tall på hvor mange brukere det innebærer.

---

[4] 'Appfail', Forbrukerrådet 2016, http://www.forbrukerradet.no/undersokelse/2015/appfail-threats-to-consumers-in-mobile-apps/ Lenke til rapport på FRs hjemmeside

[5] 'Privacy in mobile apps', SINTEF 2016 , http://www.forbrukerradet.no/undersokelse/2015/privacy-in-mobile-apps/

[6] Dette omtales i rapporten 'Appfail', kapittel 7 'Terms versus actual data flow'.

[7] http://ec.europa.eu/consumers/consumer_rights/rights-contracts/unfair-contract/index_en.htm

[8] Se mer på Runkeeper sine nettsider - https://runkeeper.com/index

[9] http://www.dinside.no/928218/de-beste-lopeappene

Appen genererer en rekke personopplysninger, eksempelvis lokasjon kombinert med tidspunkt, samt informasjon om brukerens fysiske form, helse og treningsvaner.

Sentrale dokumenter som regulerer rettsforholdet mellom app-bruker og Runkeeper:
- *Brukervilkår* datert 21. desember 2015: https://runkeeper.com/termsofservice
- *Personvernpolicy* datert 2. mars 2016, ikraft fra 1. april 2016: https://runkeeper.com/privacypolicy?showUpdatedPolicy=true

Klagepunkter

Forbrukerrådet klager her spesifikt på manglende samtykke til innhenting og deling av lokasjonsdata når appen ikke er i bruk, samt sletting. I tilknytning til samtykke vil vi likevel påpeke det grunnleggende problematiske i at Runkeeper har uklare og omfattende tillatelser og betinger seg en ensidig rett til å endre personvernpolicy uten å varsle bruker på forhånd. Det kan derfor stilles spørsmål ved om det foreligger et samtykke på tidspunktet når appen installeres og tas i bruk og ved senere endring fra Runkeeper.

1) **Runkeeper sporer brukere og sender personopplysninger til tredjepart når appen ikke er i bruk**

Undersøkelsen SINTEF gjennomførte viser at Runkeeper samler inn lokasjonsdata og sender lokasjonsdata til tredjepart når telefonen ikke er i bruk[10].

Lokasjon gir kjernefunksjonalitet i Runkeepers tjeneste og er slik sett relevant for appens formål. En trenings-app må innhente lokasjonsdata når appen er i bruk for at bruker skal kunne lagre treningsdata.

Vi stiller imidlertid spørsmål ved at treningsappen innhenter lokasjonsdata og andre personopplysninger når telefonen og appen ikke er i bruk. Vi mener videre det er problematisk at disse personopplysningene sendes til tredjepart når appen ikke er i bruk.

Vi kan ikke se at det er behov for slik lokasjonsinnhenting av hensyn til funksjonalitet i appen og stiller spørsmål ved om det er i samsvar med krav om formålsbegrensning. Vi ber derfor Datatilsynet vurdere om det er brudd på personverndirektivets krav om at personopplysninger tillates innhentet i den grad det er saklig og relevant for å utføre tjenesten[11].

Runkeeper forklarer de tekniske tilgangene de ber om. Vi finner imidlertid ikke at tjenesten på noe tidspunkt, verken inne i appen, i brukervilkår, personvernerklæring eller informasjon på nettsiden, gjør bruker oppmerksom på at lokasjon eller andre personopplysninger samles inn når telefonen ikke er i bruk, eller hentes inn når brukeren ikke er i en treningsøkt, eller at dette sendes til en tredjepart.

Lokasjon forklares slik på Runkeepers nettsider:

[10] Se faktum i saken beskrevet i vedlegget
[11] Personverndirektivet (Direktiv 95/46/EF) artikkel 6

> ***'Location:*** *We hope this one is self-explanatory, but we do in fact use your location to track your workouts. The GPS hardware exists on your phone and Runkeeper needs this permission into order to use your phone's GPS so we can be your workout buddy on the road!'*
>
> Runkeeper, understanding permissions

For en bruker er det derfor ikke selvforklarende at lokasjon spores av treningsapper og sendes til tredjeparter når brukeren ikke trener, når appen ikke er i bruk eller når telefonen ikke er i bruk.

Siden det ikke opplyses om forholdet, har heller ikke bruker gitt samtykke til at personopplysningene samles inn når appen ikke er i bruk. Vi ber derfor Datatilsynet vurdere om dette er brudd på personverndirektivets krav om at bruker må gi eksplisitt og informert samtykke til innhenting av personopplysninger[12].

Vi ser heller ikke at bruker har gitt samtykke til at lokasjon sendes tredjepart når appen ikke er i bruk. Vi ber derfor Datatilsynet vurdere om også dette er brudd på personverndirektivets samtykkekrav**.**

I denne sammenheng gjør vi Datatilsynet oppmerksom på at virker som at noe av informasjonen (som IP-adresse og enhets-ID) som deles fra Runkeeper med tredjepart ikke reguleres av Runkeepers personvernerklæring, men av tredjepartens, jf. kapittelet «Our Disclosure of Your Personal Data and Other Information»:

> *The use of online tracking mechanisms by third parties is subject to those third parties' own privacy policies, and not this privacy policy*

Det innebærer at Runkeeper ikke har ansvar for hva som skjer med når informasjon deles med tredjepart. Om dette dekker lokasjonsdata som samles inn og deles når appen ikke er i bruk er ikke klart.

2) Det er uklart om Runkeeper sletter personopplysninger rutinemessig eller når bruker ber om det

Ifølge personverndirektivet[13], skal databehandlere begrense tidsperspektivet for oppbevaring og behandling av personopplysninger. Data kan kun oppbevares så lenge det er relevant. Derfor bør ikke en app som Runkeeper oppbevare personopplysninger lenge etter at bruker har sluttet å bruke appen, eller etter at bruker har bedt om at konto slettes.

Etter det vi kan se omtaler ikke Runkeepers *personvernpolicy* eller brukervilkår hvorvidt dataoppbevaring er begrenset i tid eller om de sletter personopplysninger når bruker ber om det eller bruker sletter konto.

[12] Personverndirektivet artikkel 7
[13] Personverndirektivet artikkel 6

På nettsiden med navnet «*The Runkeeper Help Center*»[14] kan du finne opplysninger om bruk av egen Runkeeper-konto, også om hvordan en konto kan slettes. På siden med informasjon om hvordan Runkeeper-kontoen kan slettes, informeres du om at data tapes og at bruker ikke kan få tilgang til disse på nytt når kontoen slettes. Det står altså ikke noe om at opplysningene slettes, bare at bruker ikke lenger får tilgang på opplysningene.

Forbrukerrådet vil derfor anmode om at Datatilsynet undersøker om Runkeeper oppfyller personvernkrav med hensyn til sletting av personopplysninger.

Vennlig hilsen
Forbrukerrådet

Finn Myrstad
Fagdirektør Digitale tjenester
Finn.myrstad@forbrukerradet.no

[14] https://support.runkeeper.com/hc/en-us/articles/201109826-How-to-delete-your-Runkeeper-Account

Vedlegg

Oppsummering av funn gjort av SINTEF – 48-timers testen - Runkeeper

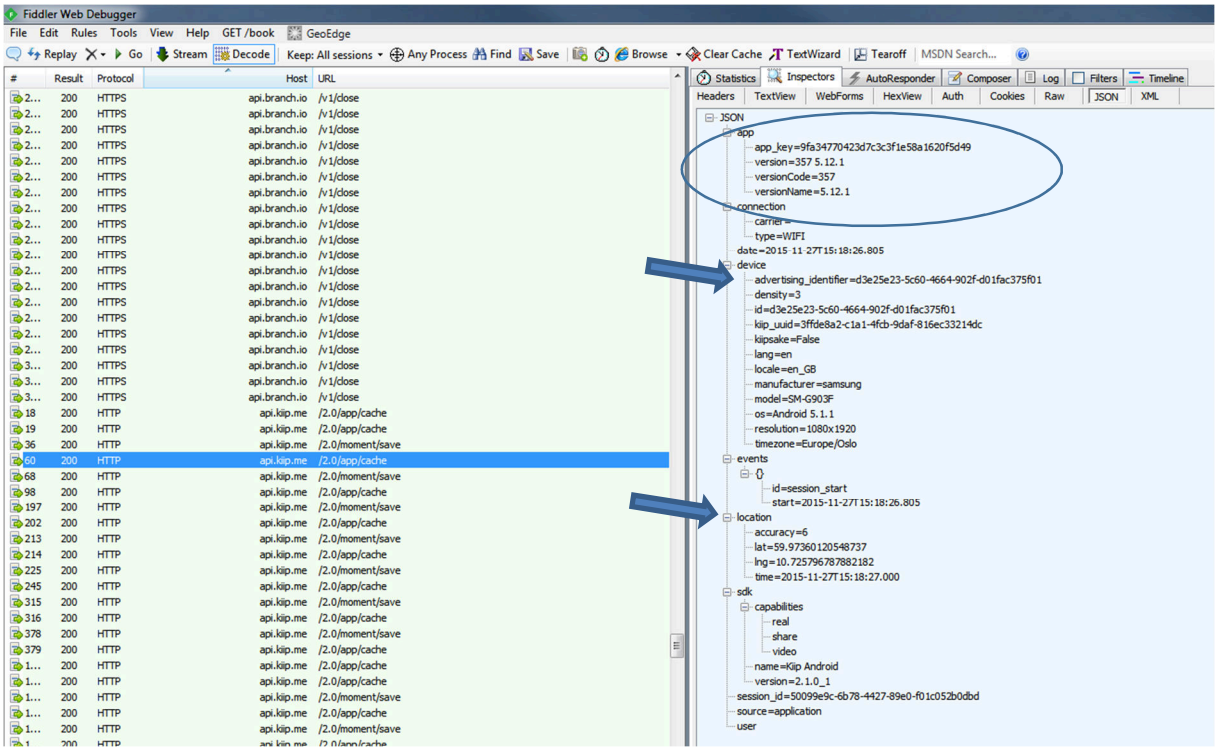
Rapporten fra SINTEF konkluderer med at Runkeeper sender lokasjon når telefonen ikke er i bruk:

> *'we also detected that GPS location was sent by MyFitnessPal and Runkeeper when the app was not in use. The user can then be geo-tracked whenever the GPS function is turned on'.*
>
> *Privacy in Mobile Apps, SINTEF,*

Bakgrunn:

SINTEF påviser at appen Runkeeper sender personopplysninger som lokasjon kombinert med tidspunkt og Google Advertising ID til tredjeparten Kiip.me når appen er i bruk (se skjermdump fra dataflyten i skjermdump 1)[15]. Bruk av lokasjon når brukeren trener er forståelig ut i fra appens funksjonalitet og omtales i personvernvilkår, selv om Kiip.me ikke omtales spesielt.

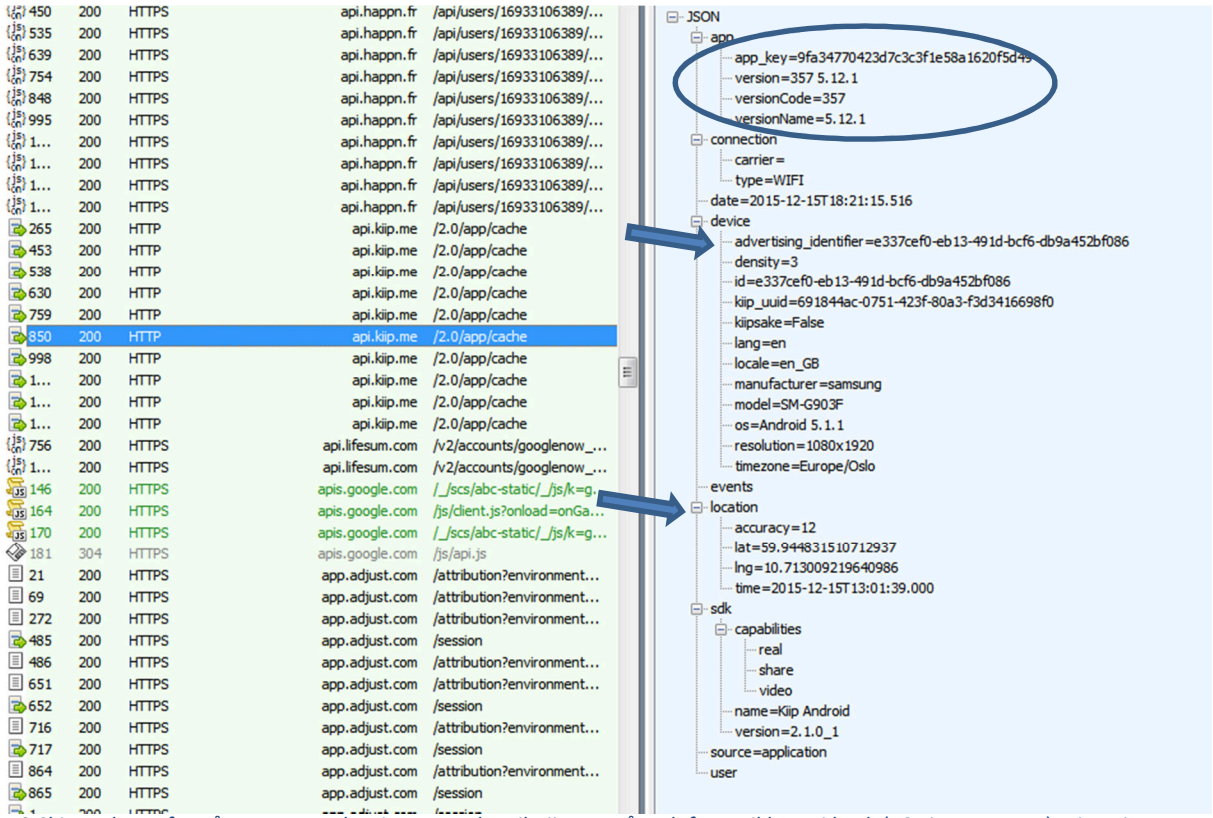
Forbrukerrådet har ikke vurdert om sending av personopplysninger til Kiip.me er problematisk i seg selv. Når vi likevel nevner det, er det fordi det at opplysningene sendes når appen er i bruk, har gjort det mulig å påvise at det er Runkeeper som sender personopplysninger til tredjepart når appen ikke er i bruk.



[15] Vi har lagt til grunn vår tolkning av Article 29 Data Protection Working Party, 'Opinion 4/2007 on the consept of personal data' når vi definerer lokasjon og advertising id som personopplysninger.

1 Skjermdump fra dataflyt fra Runkeeper da appen var i bruk. Ring viser app-identifikatorer, piler viser personopplysninger.

SINTEF påviste videre at en av de 20 appene sender en kombinasjon av personopplysninger, inklusive eksakt lokasjon, tidspunkt og Google Advertising ID til Kiip.me ti ganger i løpet av 48-timerstesten. I 48-timerstesten var telefonen ikke i bruk i 48 timer. (Se skjermdump 2 som dokumenterer hvilke data som ble sendt til Kiip.me i løpet av 48-timerstesten).



2 Skjermdump fra når personopplysninger sendes til Kiip.me når telefonen ikke er i bruk (48-timerstesten). Ring viser app-identifikatorer, piler viser personopplysninger.

At kombinasjon lokasjon og tidspunkt sendes 10 ganger i løpet av 48 timer kan i seg selv identifisere en bruker. Google Advertising Id er også personopplysninger da det er en identifikator som består fram til bruker eventuelt velger å aktivt endre den, noe få gjør[16]. Det er mulig at flere av opplysningene kan regnes som personopplysninger, men det har vi ikke vurdert, da vi anser det som helt klart at det ble sendt personopplysninger[17].

[16] At 'advertising id' ikke er identiske i de to skjermdumpene, skyldes at testen når appen var i bruk og ikke i bruk ble gjort fra to ulike brukerkontoer.

[17] 'Even if the user periodically changes his or her pseudonymous GAID [Google Advertising ID], sparse trajectories—e.g., work-home location pairs—are known to be strongly identifying and allow the advertiser to link old and new GAID, effectively turning GAID into a permanent identifier.', 'What Mobile Ads Know About Mobile Users', 2016, Son, Kim & Shmatikov, page 8: https://www.ftc.gov/system/files/documents/public_comments/2015/09/00006-97209.pdf

SINTEF gjennomførte 48-timerstesten da alle de 20 appene var på telefonen. Vi kan imidlertid fastslå at det er Runkeeper som sendte personopplysinger til tredjepart i løpet av 48-timerstesten på grunn av appidentifikatorene.
Meldingene mellom Runkeeper og Kiip.me når appen var i bruk inneholdt **identiske app-identifikatorer** som i meldingene til Kiip.me da telefonen ikke var i bruk. Dette gjelder 'app_key', som er en unik app identifikator med om lag 30 bokstaver og tall, 'version' (7 siffer),' versionCode' (3 siffer) og 'versionName' (4 siffer) (innringet på skjermdump 1 og 2). Vi viser at opplysningene ble sendt gjennom appen Runkeeper også da appen ikke var i bruk.

Det er også flere andre faktum som peker i retning av at det var Runkeeper som sendte personopplysninger til Kiip.me når telefonen ikke var i bruk. Runkeeper var den eneste **applikasjonen som kontaktet Kiip.me** da SINTEF testet applikasjonene én og én, og den eneste hvor SINTEF **detekterte Kiip.me i kildekode**. SINTEF har dessuten slått fast at **Runkeeper brukte GPS når telefonen ikke var i bruk**.

Vi mener ut fra ovenstående at det er dokumentert at Runkeeper sendte personopplysninger til tredjepart da appen og telefonen ikke var i bruk.

Dersom det er ønskelig kan vi tilgjengeliggjøre ytterligere bakgrunnsinformasjon. Kontakt eventuelt Gro Mette Moen på gmm@forbrukerradet.no.